Wireshark / tcpdump

eine Einführung

Ubuntu-Users Nürnberg
2010-01-15

Referent:
Bernd Strößenreuther
<ubuntuusers@stroessenreuther.net>

Lizenz

Einsatzgebiet

- Netzwerkkommunikation mitschneiden
- Problemanalyse
- werden auch von Angreifern eingesetzt
- generell: Sniffing immer mit root- / Administrator-Berechtigungen

tcpdump

- Kommandozeilentool
- kann dadurch hervorragend auch auf Servern eingesetzt werden
- Ausgabe der wichtigsten Infos zu jedem Paket in Echtzeit auf der Konsole
- Ausgabe auch als File im pcap Format
- Plattformen: Linux, diverse Unixe

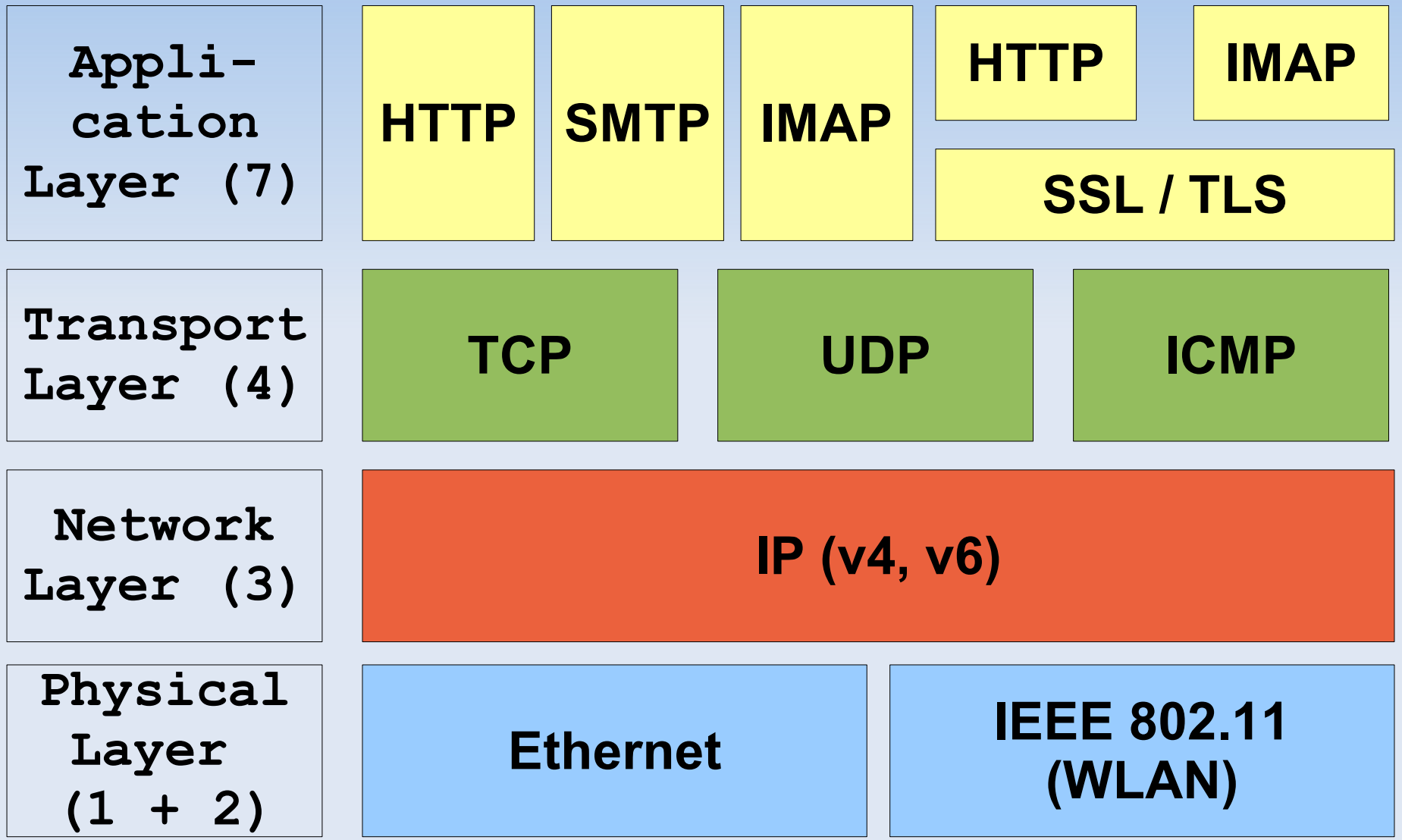
Wireshark (früher Ethereal)

- grafisches Tool
- kann selbst Netzwerkverkehr mitschneiden
- oder Files im pcap Format lesen
- deutlich erweiterte Möglichkeiten zur Analyse des mitgeschnittenen Netzwerkverkehrs gegenüber tcpdump
- Plattformen: Linux, div. Unixe, Windows
- häufige Kombination: tcpdump zum sniffen, Wireshark zur Analyse

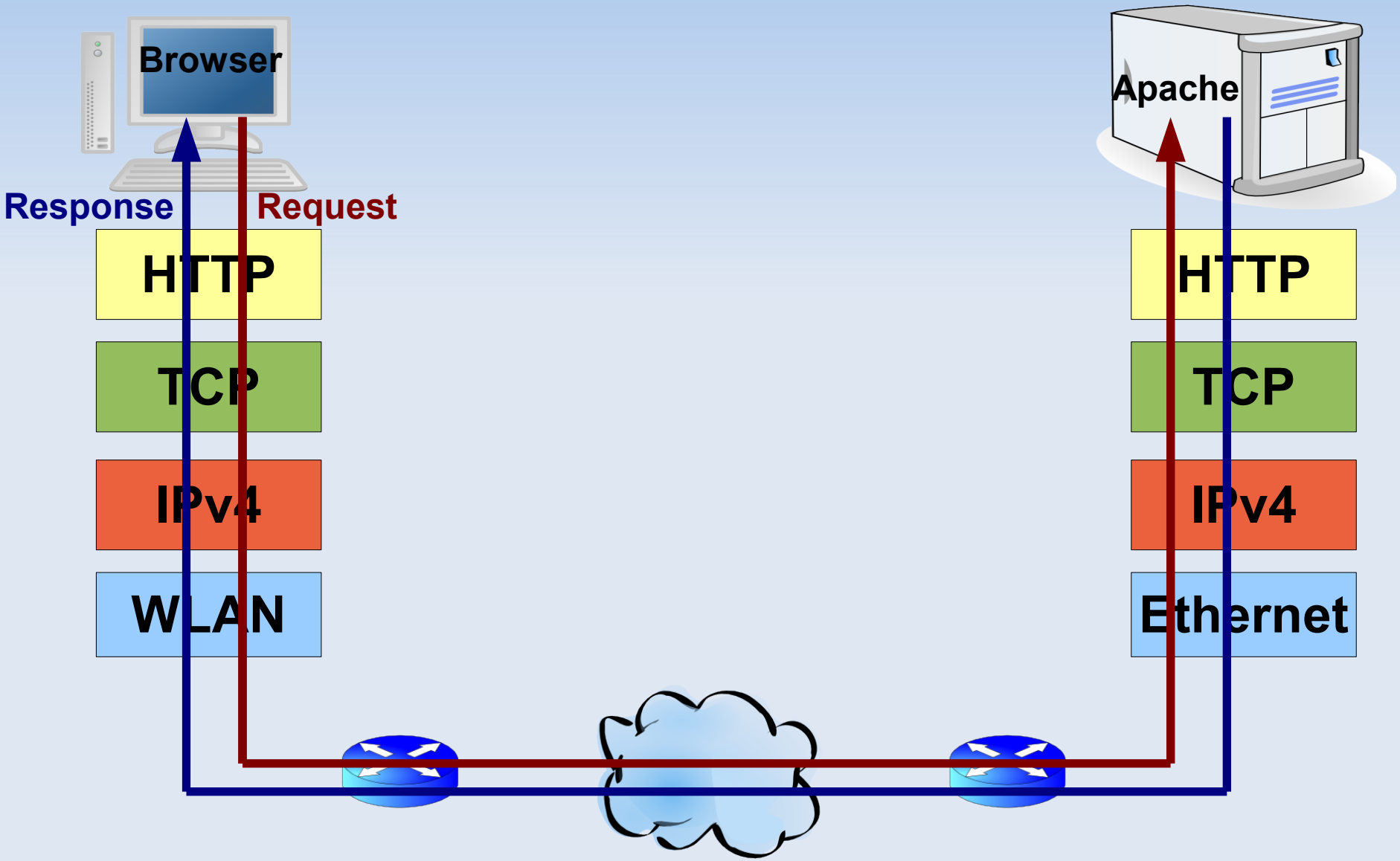
ISO-OSI-Schichtenmodell

- siehe http://de.wikipedia.org/wiki/OSI-Modell
- OSI: Open Systems Interconnection Reference Model
- ISO: International Organization for Standardization

vereinfachte Darstellung



Beispiel


Browser
Apache
Response
Request
HTTP
TCP
IPv4
WLAN
HTTP
TCP
IPv4
Ethernet

Wo sniffen?

- auf Client oder Server selbst
- auf einem Router, einem Proxy, einer Firewall auf dem Weg
- bedingt geeignet: Ein Rechner im selben LAN-Segment wie Client oder Server

Live-Demo

- alles weiter live am System...

Vielen Dank...

... für die Aufmerksamkeit

Noch Fragen?